



How to Prevent Business Email Compromise (BEC)

Information

Business Email Compromise (BEC) is one of the most financially damaging online crimes. It exploits the fact that so many of us rely on email to conduct business. In a BEC scam, the fraudster sends an email message that appears to come from a known source, thus making it appear to be a legitimate request. The fraudulent email (there are different scenarios) requests that funds be sent via Wire or ACH. By making a simple call-back to a known phone number to verify the request, you can help prevent yourself from being a victim of BEC.

Background/Details

According to the FBI, BEC scams caused over \$2.7 billion worth of losses to businesses last year. Below are some examples for you to watch out for:

- 1 The fraudster pretends to be a vendor that you regularly deal with and sends an email with updated payment instructions to use for future invoice payments.
- 2 The fraudster pretends to be a company executive and sends an email requesting an urgent payment and explains that they can't speak to you on the phone about it.
- 3 The fraudster, pretending to be someone you know or from a company you work with, sends an email requesting you purchase dozens of gift cards for an upcoming event, party, or other occasion. The fraudster asks you to share the serial numbers so they can email them right away.

Action Required

1. Before you initiate an ACH or Wire request, please make sure you are not a victim of BEC.

Some questions to ask yourself:

- Did you receive an email/text/fax from your vendor requesting that you change bank information (account number and/or bank) to pay an invoice? If yes, did you call your vendor (known phone number) to validate the request to change bank information?
 - Did you receive an email requesting that you immediately send funds to a company/individual? Did the request state it is time-sensitive and should be kept confidential? If yes, did you call the company/individual (known phone number) to validate the request to send funds?
2. Business Email Compromise (BEC) should be discussed with your staff members regularly.

Resources

Please refer to below resources which will provide you with additional information regarding Business Email Compromise (BEC).

- 1 <https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/business-email-compromise>
- 2 <https://www.bankofhope.com/privacy-and-security/online-security-information>
- 3 The Fraud Awareness and Protection Checklist includes under "Transaction Protection" best practices on how to help prevent Business Email Compromise (BEC). Contact your local Bank of Hope branch office for our Fraud Awareness and Protection Checklist.

Questions

If you have any questions regarding Business Email Compromise (BEC), please contact **Global Treasury Management Solutions** at tmsoperations@bankofhope.com or 1-800-788-4580.